5 FAM 800
INFORMATION SYSTEMS MANAGEMENT

5 FAM 810
MANAGING INFORMATION SYSTEMS

(CT:IM-159;   01-27-2015)
(Office of Origin: IRM/BMP/GRP/GP)

5 FAM 811 GENERAL

(CT:IM-115;   04-25-2011

This chapter series establishes policies for operating and managing IT operating environments abroad and domestically in the Department of State to include coordination and direction for enterprise desktop support services to IT Consolidated (ITC) bureaus and helpdesk operations for facilities at all posts. This policy applies to all personnel involved with the IT lifecycle for all systems, software controls, contingency plans, hardware and software maintenance, networks, data integrity, and logistical access controls.

5 FAM 812 SCOPES

(CT:IM-106;   06-05-2009)

The chapter discusses definitions and responsibilities for managing Information Systems, IT Services Center, software controls, continuity of operations, hardware and software maintenance, and networks.

5 FAM 813 AUTHORITIES

(CT:IM-159;   01-27-2015)

The authorities for these policies and procedures are:

(1) Paperwork Reduction Act of 1995, Public Law 104-13, 44 U.S.C. ch. 35;

(2) Information Technology Management Reform Act of 1996; (ITMRA)(Clinger-Cohen Act); Public Law 104-106; section 5001 et seq.;

(3) OMB Circular A-130, revised November 28, 2000;

(4) Presidential Decision Directive (PDD) 63, May 22, 1998;

(5) Federal Acquisition Regulation (FAR), Part 39, 48 CFR Part 39;

(6) Government Performance and Results Act of 1993, Public Law 103-62;

(7) Federal Information Security Management Act (FISMA), (Public Law 107-347, Title III);

(8) OMB Quality of Information Guidelines, 67 FR 8451-8462 (Feb. 22, 2002);

(9) Federal Records Act;

(10) Privacy Act;

(11) Executive Order 13526 - Classified National Security Information;

(12) Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems;"

(13) Federal Information Processing Standards (FIPS) Publication 200, "Minimum Security Requirements for Federal Information and Information Systems;"

(14) Committee for National Security Systems Instruction 4009 (CNSSI-4009), "National Information Assurance (IA) Glossary" (http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf);

(15) National Institute of Standards and Technology (NIST) Special Publication 800-41, "Guidelines on Firewalls and Firewall Policy;" and

(16) National Institute of Standards and Technology (NIST) Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."

5 FAM 814 DEFINITIONS

(CT:IM-159; 01-27-2015)

The following definitions apply when used in this policy:

Authorization: The formal approval of an IT system to process, store, or transmit information granted by a management official. Authorization, which is required under OMB Circular A-130, is based on an assessment of the management, operational, and technical controls associated with an IT system.

Certification: The comprehensive evaluation of the technical and non-technical security controls of an IT system to support the authorization process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

ClassNet: A physical and logical Internet Protocol (IP)-based global network that links the Department of State's domestic sites and embassies, consulates, and annexes abroad for communications up to and including the Secret level of classification.

Cyber Security: Information operations that protect and defend information and

IT systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of IT systems by incorporating protection, detection, and reaction.

Dedicated Internet Network (DIN): Dedicated Internet access from an Internet Service Provider (ISP) on a discrete local area network (LAN) that is not connected to any other Department system.

Demilitarized Zone (DMZ): *Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.*

Designated Approval Authority (DAA): The person formally authorized to assume responsibility for operating a system at an acceptable level of risk. For the Department of State, the Chief Information Officer (CIO) is the DAA, except in the case of SCI (see 1 FAM 270). This term is synonymous with designated accrediting authority and delegated accrediting authority.

Domestic Information Systems Security Officer (DISSO): The DISSO provides desktop security support and fulfills Information Systems Security Officer (ISSO) responsibilities with regard to maintaining requirements for all desktops and providing desktop security guidance to all users within bureaus that have fully consolidated– as defined in by the respective Master Service Level Agreement (SLA) for each consolidated bureau and ISSO appointment memo.

Information Security Steering Committee: As defined in 5 FAM 119, the Information Security Steering Committee (ISSC) was established by the Undersecretary for Management (M) in 2005. The ISSC is a Department-wide Deputy Assistant Secretary-level group consisting of owners of information systems. The ISSC is co-chaired by the Chief Information Security Officer and the Senior Coordinator for Security Infrastructure.

Information Technology System (IT System): As defined in OMB Circular A-130, a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with procedures, whether automated or manual.

Information Systems Security Officer (ISSO): As defined in 5 FAM 824, the person responsible to the system/data owner for overseeing that security requirements are addressed for an IT system throughout its lifecycle, from design through disposal.

Information Technology Asset Baseline (ITAB): The repository for information on all Department applications. This is the official source of external reporting regarding the Department's application portfolio.

Information Technology Asset Management (ITAM): IT asset management brings together physical, financial, and contractual management of IT assets in order to drive costs down and improve service levels. Managing the physical aspects of a technology asset portfolio can provide insight about what assets are in your environment, where they are physically located, to whom they are assigned, and to what extent they are being used.

Information Technology *Configuration* Control Board (IT CCB)**:** The entity that manages hardware, software, and hardware/software configuration changes to the Department's global IT environment. The IT CCB has responsibility for reviewing and approving/disapproving changes that potentially affect the Department's global IT environment. The scope includes software and hardware products residing on unclassified, Sensitive but Unclassified (SBU), and classified infrastructures (stand-alone or networked) up to and including the Secret level of classification.

Local Area Network (LAN): A number of interconnected data communication protocols and devices joining a wide variety of devices such as computers, printers, storage devices, and other peripheral equipment within a single building or a campus of buildings. LANs provide the capability to share files and other resources among multiple users.

Local *Configuration* Control Board (Local CCB): A formally constituted group of stakeholders responsible for maintaining control of their own hardware and software change processes within the bounds of the IT CCB Standard Operating Procedure.

OpenNet: A physical and logical Internet Protocol (IP)-based global network that links the Department's domestic sites and embassies, consulates, and annexes abroad at the Sensitive but Unclassified level.

Plan of Action and Milestones (POA&M): A remediation tool that contains the actions necessary to correct system security weaknesses.

Remedy: A Web-enabled incident/problem reporting and tracking system used by IRM. A single form is used to enter a trouble ticket, a unique ticket number is automatically assigned when the ticket is successfully submitted, and tickets are stored in one universal database. The IT Service Center creates Remedy tickets and transfers tickets they cannot resolve to Tier II/III action offices. Tier II/III action offices provide skilled technical support in specific areas.

Risk Management: The total process of identifying, controlling, and mitigating IT system-related risks. It includes risk assessment; cost benefit analysis; and the selection, implementation, test, and security evaluation of security controls. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws.

Stand-Alone: A device that functions independently of a network.

Support System: An interconnected set of information resources under the same direct management control and sharing common functionality.

System Authorization Plan (SAP): A comprehensive and uniform approach to the System Authorization Process that is comprised of four phases: Phase 1 – Precertification; Phase 2 – Certification; Phase 3 – Authorization; and Phase 4 – Post-Authorization.

System Owner: The Bureau Executive is the owner of locally developed systems. At the post level the Deputy Chief of Mission (DCM) may assume this responsibility. They are responsible for the IT system for the entire system lifecycle. The System Owner is concerned with cost, schedule, and performance issues for the system as well as security issues and represents the interests of the user community and the IT system throughout the system lifecycle.

System Security Plan: A plan used in the system authorization process to document a system's security controls as identified in the system baseline and to verify each control as implemented, partially implemented, or not applicable.

Unauthorized Disclosure of Passwords: The release of password information to persons other than senior IT management or security personnel for purposes of performing an investigation.

Wide Area Network (WAN): A data communication function that connects geographically disparate Local Area Networks using long-haul networking facilities and protocols.

5 FAM 815 THROUGH 819 UNASSIGNED